CLAIMS

[1] A secure system including a secure device holding confidential data and a terminal apparatus to which said secure device is connected, said secure system comprising:

5   a first storage unit included in one of said secure device and said terminal apparatus, and operable to store domain information defining a domain of said secure device and said terminal apparatus;

a second storage unit included in one of said secure device and said terminal apparatus, and operable to store an extra-domain

10 usage rule which is a rule for use of said secure device outside the domain;

a first judgment unit included in one of said secure device and said terminal apparatus, and operable to judge, according to the domain information, whether one of said secure device and said

15 terminal apparatus is currently inside the domain or outside the domain;

a second judgment unit included in one of said secure device and said terminal apparatus, and operable to judge, according to the extra-domain usage rule, whether or not use of said secure device is

20 permitted, in the case where it is judged by said first judgment unit to be outside the domain; and

a control unit included in one of said secure device and said terminal apparatus, and operable to enable the use of said secure device in said terminal apparatus in any of: the case where it is

25 judged by said first judgment unit to be inside the domain; and the case where it is judged by the second judgment unit that use is permitted.

[2] The secure system according to Claim 1,

30 wherein said terminal apparatus is a content use apparatus reproducing an encrypted content,

the confidential data is an encryption key for decrypting the

content, and

said control unit is operable to supply the confidential data from said secure device to said terminal apparatus, in any of: the case where it is judged by said first judgment unit to be inside the domain; and the case where it is judged by said second judgment unit that use is permitted.

[3]   The secure system according to Claim 2,

wherein the extra-domain usage rule concerns at least one of the following extra-domain criteria: (a) the number of content reproductions; (b) the number of content use apparatuses; (c) the number of domains; (d) a validity period; (e) a use duration; (f) the number of terminal IDs; (g) the number of domain IDs; (h) the number of contents; and (i) the number of licenses.

[4]   The secure system according to Claim 2, comprising

a history recording unit operable to record an extra-domain use history indicating a history of use of the content in a content use apparatus outside of the domain, the use being based on the extra-domain usage rule,

wherein said second judgment unit is operable to judge whether or not the extra-domain use history exceeds a limit of permitted use indicated in the extra-domain usage rule.

[5]   The secure system according to Claim 2,

wherein said second storage unit and said second judgment unit are included in said secure device.

[6]   The secure system according to Claim 2,

wherein said second storage unit and said second judgment unit are included in said content use apparatus.

[7] The secure system according to Claim 2,

wherein said content use apparatus includes

a reception unit operable to receive a new extra-domain usage rule from an outside source, and

5 said second storage unit is operable to update the extra-domain usage rule with the new extra-domain usage rule.

[8] The secure system according to Claim 7,

wherein said reception unit is operable to receive an

10 extra-domain usage rule added to a license transmitted by a content distribution server.

[9] The secure system according to Claim 2,

wherein said content use apparatus further includes:

15 an obtainment unit operable to obtain the extra-domain usage rule and an extra-domain use history from a secure device inserted into a secure device slot; and

a display unit operable to display a guidance regarding a use status for a content use apparatus outside of the domain, based on

20 the obtained extra-domain usage rule and the extra-domain use history.

[10] A secure device connected to a terminal apparatus, and holding confidential data, said secure device comprising:

25 a rule storage unit operable to store an extra-domain usage rule for said secure device with respect to a terminal apparatus outside of a domain;

a judgment unit operable to judge, according to the extra-domain usage rule, whether or not use of said secure device is

30 permitted; and

a control unit operable to enable the use of said secure device in said terminal apparatus in the case where said judgment unit

judges that the use is permitted.

[11]　The secure system according to Claim 10,

wherein said terminal apparatus is a content use apparatus
reproducing an encrypted content,

the confidential data is an encryption key for decrypting the
content, and

said control unit is operable to supply the confidential data
from said secure device to said terminal apparatus, in the case
where it is judged by said judgment unit that use is permitted.

[12]　The secure device according to Claim 11,

wherein the extra-domain usage rule concerns at least one of
the following: (a) the number of content reproductions; (b) the
number of content use apparatuses; (c) the number of domains; (d)
a validity period; (e) a use duration; (f) the number of terminal IDs;
(g) the number of domain IDs; (h) the number of contents; and the
number of licenses.

[13]　The secure device according to Claim 12,

a history recording unit operable to record an extra-domain
use history indicating a history of use of the content in a terminal
apparatus outside of the domain, the use being based on the
extra-domain usage rule,

wherein said judgment unit is operable to judge whether or
not the extra-domain use history exceeds a limit of permitted use
indicated in the extra-domain usage rule.

[14]　The secure device according to Claim 13, further comprising
a deleting unit operable to delete the extra-domain use
history at a predetermined time.

[15]   The secure device according to Claim 11, further comprising:

a reception unit operable to receive a new extra-domain usage rule from a terminal apparatus,

wherein said rule storage unit is operable to update the extra-domain usage rule with the new extra-domain usage rule.

[16]   The secure device according to Claim 11,

wherein said rule storage unit is operable to store a default extra-domain usage rule.

[17]   The secure device according to Claim 11, further comprising:

a display unit operable to display a use status for a content use apparatus outside of the domain, based on the extra-domain usage rule and the extra-domain use history.

[18]   The secure device according to Claim 11, further comprising:

a transmission unit operable to transmit a domain ID to a terminal apparatus having a secure device slot into which said secure device is currently inserted.

[19]   The secure device according to Claim 11, further comprising

a transmission unit operable to transmit the extra-domain use history to a terminal apparatus having a secure device slot into which said secure device is currently inserted.

[20]   A terminal apparatus to which a secure device holding confidential data is connected, said terminal apparatus comprising:

a storage unit operable to store an extra-domain usage rule which is a usage rule for said secure device with respect to a terminal apparatus outside the domain;

a judgment unit operable to judge, according to the extra-domain usage rule, whether or not use of said secure device is

permitted; and

a control unit operable to enable the use of said secure device in said terminal apparatus in the case where said judgment unit judges that the use is permitted.

5

[21] The secure system according to Claim 20,

wherein said terminal apparatus is a content use apparatus reproducing an encrypted content,

the confidential data is an encryption key for decrypting the content, and

10

said control unit is included in said secure device, and is operable to supply the confidential data from said secure device to said terminal apparatus, in the case where it is judged by said judgment unit that use is permitted.

15

[22] The secure device according to Claim 21,

wherein the extra-domain usage rule concerns at least one of the following: (a) the number of content reproductions; (b) the number of content use apparatuses; (c) the number of domains; (d) a validity period; (e) a use duration; (f) the number of terminal IDs;

20

(g) the number of domain IDs; (h) the number of contents; and the number of licenses.

[23] A secure system including a content distribution apparatus, a content use apparatus, and a secure device,

25

wherein said content distribution apparatus includes a transmission unit operable to transmit, to a content use apparatus, an extra-domain usage rule which is a usage rule for use of said secure device in a content use apparatus outside of a domain,

30

said secure device includes a supply unit operable to supply an encryption key to a content use apparatus belonging to a domain made up of content use apparatuses which share said secure device,

the encryption key enabling content use,

said content use apparatus includes a reception unit for receiving the extra-domain usage rule from said transmission unit,

one of said content use apparatus and said secure device includes:

a first storage unit operable to store domain information defining the domain of said secure device and said terminal apparatus;

a second storage unit operable to store the extra-domain usage rule received by said reception unit;

a first judgment unit operable to judge whether one of said secure device and said terminal apparatus is currently inside the domain or outside the domain; and

a second judgment unit operable to judge, according to the extra-domain usage rule, whether or not use of said secure device is permitted, in the case where it is judged by said first judgment unit to be outside the domain, and

said supply unit is further operable to supply the encryption key to a content use apparatus outside the domain, in the case where said judgment unit judges that the use is permitted.

[24] A method for using a secure device in a secure system including the secure device which holds confidential data, and a terminal apparatus to which the secure device is connected, said method comprising:

a step of reading-out, from a memory, domain information defining a domain of a secure device and a terminal apparatus, the memory being included in one of the secure device and the terminal apparatus;

a step of judging, according to the read-out domain information, whether one of the secure device and the terminal apparatus is currently inside the domain or outside the domain;

- 47 -

a step of reading out, from a memory, an extra-domain usage rule which is a rule for use of the secure device outside the domain, the memory being included in one of the secure device and the terminal apparatus;

5   a step of judging, according to the read-out extra-domain usage rule, whether or not use of the secure device is permitted, in the case where it is judged by said first judgment unit to be outside the domain; and

a control step of enabling use of the secure device in the
10   terminal apparatus in any of: the case where it is judged to be inside the domain; and the case where it is judged that use is permitted.

[25]   The secure device use method according to Claim 24,

wherein the terminal apparatus is a content use apparatus
15   reproducing an encrypted content,

the confidential data is an encryption key for decrypting the content, and

in said control step, the confidential data, within the secure device, is supplied from the secure device to the terminal apparatus
20   in any of: the case where it is judged by the first judgment unit to be inside the domain; and the case where it is judged by the second judgment unit that use is permitted.

[26]   A computer executable program for use in a secure system
25   including a secure device which holds confidential data, and a terminal apparatus to which the secure device is connected, said program causing a computer to execute:

a step of reading-out, a memory, domain information defining a domain of a secure device and a terminal apparatus, the memory
30   being included in one of the secure device and the terminal apparatus;

a step of judging, according to the read-out domain

information, whether one of the secure device and the terminal apparatus is currently inside the domain or outside the domain;

a step of reading out, a memory, an extra-domain usage rule which is a rule for use of the secure device outside the domain, the memory being included in one of the secure device and the terminal apparatus;

a step of judging, according to the read-out extra-domain usage rule, whether or not use of the secure device is permitted, in the case where it is judged by the first judgment unit to be outside the domain; and

a control step of enabling use of the secure device in the terminal apparatus in any of: the case where it is judged to be inside the domain; and the case where it is judged that use is permitted.

[27]   A content distribution apparatus in a content use system including said content distribution apparatus, a content use apparatus, and a secure device, said content distribution apparatus comprising

a transmission unit operable to transmit, to a content use apparatus, an extra-domain usage rule which is a usage rule for said secure device with respect to a content use apparatus outside of a domain.

[28]   The content distribution apparatus according to Claim 27, wherein the extra-domain usage rule concerns at least one of the following extra-domain criteria: (a) the number of content reproductions; (b) the number of content use apparatuses; (c) the number of domains; (d) a validity period; (e) a use duration; (f) the number of terminal IDs; (g) the number of domain IDs; (h) the number of contents; and the number of licenses.